D-MATH Algebra I HS18
Prof. Rahul Pandharipande

Solution 14

FINITELY GENERATED MODULES OVER A PID, ELEMENTARY DIVISORS

1. Consider the abelian group

$$A = \mathbb{Z}/250\mathbb{Z} \times \mathbb{Z}/275\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.$$

   (a) Express A as a product of p-primary abelian groups.
   (b) Express A in terms of elementary divisors.

   Solution:

   (a) First we compute the prime decompositions

$$250 = 2 \cdot 5^3,\ 275 = 5^2 \cdot 11,\ 24 = 3 \cdot 2^3,\ 9 = 3^2.$$

   Applying the Chinese Remainder Theorem to each factor of A and reordering the factors, we obtain the decomposition

$$A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5^3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}.$$

   (b) For each prime, at most two powers of it appear in the decompositions of A computed above. Hence we get two elementary divisors. The biggest is the product of the highest prime powers of each prime, that is, $d_2 = 2^3 \cdot 3^2 \cdot 5^3 \cdot 11 = 99000$. The remaining prime power, multiplied together, give us $d_1 = 2 \cdot 3 \cdot 5^2 = 150$. Hence,

$$A \cong \mathbb{Z}/150\mathbb{Z} \times \mathbb{Z}/99000\mathbb{Z}.$$

2. Let $m, n \in \mathbb{Z}_{>0}$ and $A = (a_{ij}) \in M_{m,n}(\mathbb{Z})$ and

$$u : \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$$

   the corresponding $\mathbb{Z}$-linear map.

   (a) Show that $\mathbb{Z}^m/\mathrm{Im}(u)$ is finite if and only if A has rank m in $M_{m,n}(\mathbb{Q})$.
   (b) Suppose that $m = n$ and that $\mathbb{Z}^n/\mathrm{Im}(u)$ is finite. Prove

$$|\det(A)| = \mathrm{Card}(\mathbb{Z}^n/\mathrm{Im}(u)).$$

(c) Let $m = n = 3$. Consider the $\mathbb{Q}$-linear map $v : \mathbb{Q}^3 \longrightarrow \mathbb{Q}^3$ whose corresponding matrix (with respect to the standard basis) is

$$A = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 3 \\ 4 & 1 & 1 \end{pmatrix}.$$

Let $X = \{(x_1, x_2, x_3) \in \mathbb{Q}^3 : 0 \leqslant x_j < 1\}$. Compute the number of points of $v(X)$ having integer coordinates [*Hint:* Let u be the map $\mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ defined by the same matrix. Define a bijection between $v(X) \cap \mathbb{Z}^3$ and $\mathbb{Z}^3/\mathrm{Im}(u)$.]

Solution:

(a) By the classification of free $\mathbb{Z}$-modules, we know that $\mathbb{Z}^m/\mathrm{Im}(u)$ is finite if and only if it has rank 0. As seen in class, this submodule has rank $m - \dim_{\mathbb{Q}}(Im(v))$, where $v : \mathbb{Q}^n \longrightarrow \mathbb{Q}^m$ is the $\mathbb{Q}$-linear map given by the matrix A as well. Hence $\mathbb{Z}^m/\mathrm{Im}(u)$ is finite if and only if v is surjective, which by linear algebra is the case if and only if A has rank m in $M_{m,n}(\mathbb{Q})$.

(b) As seen in class, we can perform basic row and columns transformations in order to transform A into a matrix B of the form:

$$B = \mathrm{diag}(d_1, d_2, \ldots, d_n).$$

where $d_j \in \mathbb{Z}$ and $d_j | d_{j+1}$ for all $j = 1, \ldots, n-1$. Those operations preserve the determinant, meaning that $\det(A) = \det(B)$. Moreover, if we denote by $u_B : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ the $\mathbb{Z}$-linear map defined by B, then $\mathbb{Z}^n/\mathrm{Im}(u) \cong \mathbb{Z}^n/\mathrm{Im}(u_B)$, so that in particular the two groups have the same cardinality. All integers d_j are non-zero, because otherwise the matrix B would have rank strictly smaller n, so that $\mathbb{Z}^n/\mathrm{Im}(u_B)$ would not be finite. Now, $\mathbb{Z}^n/\mathrm{Im}(u_B) \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$ has cardinality $\prod_j d_j = \det(B)$ because $d_j \neq 0$ for all j, so that $\det(A) = \mathrm{Card}(\mathbb{Z}^n/\mathrm{Im}(u))$.

(c) The given matrix A is non-singular, since $\det(A) = 7 \neq 0$. Hence the map v is bijective. Consider the composition of maps $\varphi : v(X) \cap \mathbb{Z}^3 \hookrightarrow \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3/\mathrm{Im}(u)$, where the latter is the natural projection. We claim that this is a bijection.

First, let us check injectivity. For $y_1, y_2 \in v(X) \cap \mathbb{Z}^3$, there exist unique $x_1, x_2 \in \mathbb{Q}^3$ such that $v(x_j) = y_j$, and it must be the case that $x_1, x_2 \in X$. The coordinates of $x_1 - x_2$ are bound to have absolute value strictly smaller than one. If $\varphi(y_1) = \varphi(y_2)$, then $v(x_1 - x_2) = y_1 - y_2 \in \mathrm{Im}(u)$, which is equivalent to $x_1 - x_2 \in \mathbb{Z}^3$, which by assumption is only possible for $x_1 = x_2$, implying $y_1 = y_2$. This proves injectivity of φ.

Conversely, let $y \in \mathbb{Z}^3$ and $x \in \mathbb{Q}^3$ the unique element such that $v(x) = y$. We can uniquely decompose $x = x_0 + x_1$ for $x_0 \in X$ and $x_1 \in \mathbb{Z}^3$. Then

$v(x) - v(x_0) = v_(x_1) \in \mathrm{Im}(u)$, so that y is equivalent to $v(x_0) \in v(X) \cap \mathbb{Z}^3$ in $\mathbb{Z}^3/\mathrm{Im}(u)$.

Using bijectivity of φ and the previous part, we can conclude that the number of in $v(X)$ with integer coordinates is

$$\mathrm{Card}(v(X) \cap \mathbb{Z}^3) = \mathrm{Card}(\mathbb{Z}^3/\mathrm{Im}(u)) = |\det(A)| = 7.$$

3. Let $A = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z}$ with $1 < d_1|d_2|\ldots|d_m$. Show that any generating set of A has $\geqslant m$ elements.

   Solution: Let p be a prime dividing d_1 and suppose that $g_1, \ldots, g_n$ are generators of A. Write $d_j = p^{e_j}k_j$ with $p \nmid k_j$. Then $\pi : A \longrightarrow A_p$ is a surjective map, and $\pi(g_1), \ldots, \pi(g_n)$ are generators of

   $$A_p \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_m}\mathbb{Z}.$$

   The abelian group A_p/pA_p is a $\mathbb{Z}/p\mathbb{Z}$-vector space, because $p\mathbb{Z}$ acts trivially on it. The classes of $\pi(g_1), \ldots, \pi(g_n)$ modulo pA_p are not only $\mathbb{Z}$-generators of A_p/pA_p, but $\mathbb{Z}/p\mathbb{Z}$-generators as well. Moreover (the big fraction in the following denotes a quotient group), there are isomorphisms of $\mathbb{Z}/p\mathbb{Z}$-vector spaces

   $$A_p/pA_p \cong \frac{\mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_m}\mathbb{Z}}{p\mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times p\mathbb{Z}/p^{e_m}\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z} \times \ldots \mathbb{Z}/p\mathbb{Z} = (\mathbb{Z}/p\mathbb{Z})^m,$$

   so that $\dim_{\mathbb{Z}/p\mathbb{Z}}(A_p/pA_p) = m$ and $n \geqslant m$ by basic linear algebra.

4. Let K be a field and $E = K[X]/gK[X]$, for some $g \in K[X]$ of degree $d := \deg(g) \geqslant 1$. Consider the K-linear map $u : E \longrightarrow E$ sending $[f] \mapsto [X \cdot f]$.

   (a) Compute the matrix of u in the basis $1, X, \ldots, X^{d-1}$.

   (b) Compute the characteristic polynomial of u.

   Solution:

   (a) Write $g = \sum_{k=0}^{d} a_k X^k$ for $a_k \in K$, with $a_d \neq 0$. The map u sends $X^k \mapsto X^{k+1}$ for $k = 0, \ldots, d-2$, and $X^{d-1} \mapsto X^d = -\sum_{k=0}^{d-1} a_d^{-1} a_k X^k$. Hence the matrix of u is

   $$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -\frac{a_0}{a_d} \\ 1 & 0 & \ldots & 0 & -\frac{a_1}{a_d} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -\frac{a_{d-1}}{a_d} \end{pmatrix}$$

(b) The characteristic polynomial can be computed using the Lagrangian expansion along the last column of $A - I \cdot X$:

$$\chi_u = \sum_{j=0}^{d-2} (-1)^{d+j-1} \frac{-a_j}{a_d} (-X)^j = \frac{(-1)^d}{a_d} g.$$

5. Find the abelian group G having generators a, b, c and relations

$$\begin{aligned} -6a - 12b + 2c &= 0, \\ 7a + 8b + 7c &= 0, \\ -3a - 8b + 5c &= 0. \end{aligned}$$

[*Hint:* Work as in Example B-3.88 in J. Rotman, "Advanced modern algebra, 3rd edition, part 1".]

Solution: By elementary row and column operations, we can transform

$$\begin{pmatrix} -6 & -12 & 2 \\ 7 & 8 & 7 \\ -3 & -8 & 5 \end{pmatrix} \longrightarrow \cdots \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 8 \end{pmatrix}$$

Then (see reference in the hint) $G \cong \mathbb{Z}/1\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.